UNIVERSIDAD DE COSTA RICA

Centro de Informática
Universidad de Costa Rica

FirmaDigital

Manual de instalación, configuración y firma de documentos con firma digital avanzada XADES X-L

PLATAFORMA LINUX
JUNIO - 2014

Índice de contenido

1.Introducción 5

2 Definiciones 6

3 Firma Digital 9

4 Instalación del componente de firma digital para LibreOffice 12

4.1 Requisitos 12

4.2 Instalación de LibreOffice 12

4.3 Librería JSS de Mozilla Firefox 13

4.4 instalación del componente 15

5 Firma avanzada con formato "XADES X-L" 18

5.1 Firmar un documento 18

5.2 Verificar firma 22

5.2.1 Verificación general 22

5.2.2 Verificación detallada 23

5.2.3 Ver XML de la firma digital 24

6 Jerarquía Nacional de Certificados 26

7 Configuración del componente de firma digital 27

8 Errores 28

9 Referencias bibliográficas 29

Índice de ilustraciones

Ilustración 1	Firmado de un documento	10
Ilustración 2	Validez de Firma	11
Ilustración 3	Desempacar librerías	14
Ilustración 4	Ingreso de contraseña del usuario root	14
Ilustración 5	Asignación de permisos	14
Ilustración 7	Menú Herramientas LibreOffice	15
Ilustración 6	Copia de librerías adicionales	15
Ilustración 8	Opciones avanzadas de LibreOffice	15
Ilustración 9	Archivo de instalación del componente de firma digital para LibreOffice	16
Ilustración 10	Aceptar la instalación	16
Ilustración 11	Aceptar la licencia del nuevo componente	17
Ilustración 12	Espera de la instalación el componente	17
Ilustración 13	Nuevo menú en la barra de menú principal de LibreOffice	18
Ilustración 14	Selección firma XADES X-L	19
Ilustración 15	Ventana principal de Firma Digital	19
Ilustración 16	Diálogo para ingresar la clave privada de desbloqueo de la tarjeta criptográfica	20
Ilustración 17	Ventana de selección del certificado para firmar	20
Ilustración 18	Ventana de espera mientras se firma el documento	21
Ilustración 19	Notificación de aplicación de firma digital	21
Ilustración 20	Barra de estado de LibreOffice indica y valida una firma digital	22
Ilustración 21	Ventana principal de Firma Digital, vista de un documento firmado anteriormente	23
Ilustración 22	Ventana de detalle de un firma digital seleccionada	24
Ilustración 23	Ventana ver XML, para ver la estructura interna de la firma digital	25
Ilustración 24	Ventana de información de los certificados digitales	25
Ilustración 25	Jerarquía Nacional de Certificados Digitales	26

Ilustración 26 Menú principal del componente de firma digital 27
Ilustración 27 Ventana de configuración del componente de firma digital 27
Ilustración 28 Error en el manejo de la Firma avanzada 28
Ilustración 29 Error por problemas de la zona horaria registrada en el computador 28

1.Introducción

La firma digital es una herramienta tecnológica que está incorporándose a la sociedad costarricense poco a poco. Con la aprobación de la Ley 8454 del 2005 se inicia el uso de la firma digital en Costa Rica. Distintas empresas públicas o privadas han iniciado el uso de esta tecnología para facilitar y asegurar la autenticidad de los trámites en donde anteriormente se requería la firma autógrafa de los interesados.

Por otro lado, la Universidad de Costa Rica (UCR) impulsa el uso de herramientas de software libre en la docencia, investigación y gestión administrativa, dando paso al interés de incorporar el uso de la firma digital en el quehacer diario de las gestiones institucionales.

Así es como se inicia el desarrollo de una herramienta que permite aplicar la firma digital a distintos documentos para garantizar la autoría e integridad del documento electrónico, facilitando de esta forma la gestión universitaria. Sin embargo, la herramienta debe contar con ciertas características como por ejemplo estar incorporado a un software de la categoría de procesador de texto bajo el licenciamiento de software libre, a raíz de una política institucional que incentiva el uso de herramientas de software libre en la investigación, docencia y administración.

El presente documento es una guía para el uso de la herramienta donde se incluye como temas principales :

- Conceptos generales de la firma digital.
- Instalación del componente de firma digital en plataforma Linux.
- Pasos para aplicar firma digital en un documento de LibreOffice.

2 Definiciones

CIFRADO ASIMÉTRICO: Conocido como cifrado de clave pública, según José Alcántara (especialista en software libre) es una técnica de securización de información que en lugar de proteger la información tras una clave de acceso a la misma, requiere de dos claves relacionadas entre sí. Una de las claves se usa para codificar (proteger) la información y la otra se usa para decodificar (acceder) la información previamente cifrada.

CRIPTOGRAFÍA: Es una técnica que protege documentos y datos para dar seguridad al usuario y preservar la integridad de la web. Su funcionamiento se basa en la utilización de cifras o códigos aplicados a documentos confidenciales que circulan en la red (INFORMATICAHOY).

DIGESTO: Es una "huella digital" (Trajtenberg, 2002) del documento, construida con toda la información del mensaje. El tamaño no varía con respecto a la longitud del mensaje. Sin embargo, con un solo cambio en el texto original, el algoritmo alterará el resultado final.

LLAVE PÚBLICA Y LLAVE PRIVADA: Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, así no es posible que dos personas hayan obtenido la misma pareja de claves.

MD5: Según Iván Martínez (2013), es un algoritmo que proporciona un código (también llamado *hash*) asociado a un archivo o texto concreto. Es utilizado en el mundo del software como seguridad para que el archivo descargado no sea alterado, dandole confianza al usuario que el archivo es igual al publicado por el desarrollador (Wikipedia, 2014).

NO REPUDIO: Dividida en dos según Firma Digital.cr: no repudio del usuario y no repudio del sistema. En el modo usuario, este no puede negar que él realizó una transacción firmada digitalmente ya que solo él posee el certificado digital con la llave privada con que se generó la firma digital. El modo de sistema indica que es posible que se genere un recibo firmado digitalmente de la transacción recibida; esta servirá como prueba de transacción.

OPENDOCUMENT:

Es un estándar de documentos de datos, enfocado a las aplicaciones ofimáticas que permite interpretar correctamente los documentos creados con cualquier aplicación de ofimática. El ODF fue aprobado como estándar OASIS (Formato de Documento Abierto para Aplicaciones Ofimáticas) en el 2005 (Gobierno de España, 2008).

OCSP:

Online Certificate Status Protocol RFC 2560, permite validar el estado de un certificado digital de forma eficiente con el fin de no utilizar Listas de Revocación de Certificados -CRL (CATCert).

RFC 2560:

Es un documento de internet donde se especifica el protocolo OCSP, utilizado para el estado de revocación de un certificado digital.

SHA:

El Algoritmo de Hash Seguro (*Secure Hash Algorithm*) es un sistema de funciones hash criptográficas relacionadas. Una función *hash* es "como una firma para un texto o fichero" indica Preukschat. Este algoritmo criptográfico, transforma un mensaje en una serie ilegible aleatoria, usando una clave de encriptación que puede obtener el mensaje original solo por quienes conocen dicha clave. La encriptación permite enviar públicamente por internet la información privada sin riesgo.

X.509:

Es un estándar desarrollado por UIT-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization/International Electrotechnical Commission*) para definir el formato de certificados digitales. Incluye infraestructuras de claves públicas (en inglés, *Public Key Infrastructure o PKI*). Permitiendo delimitar el tiempo de validez, información sobre la Autoridad de Certificación que lo ha generado y otros datos para la gestión y control (Banco Santander).

XADES-XL:

La Firma electrónica avanzada XML (XML Advanced Electronic Signatures) es un conjunto de extensiones a las recomendaciones XML-Dsig adecuadas a las firma electrónica avanzada. Xades define seis perfiles según el nivel de protección, XADES X-L es uno de ellos que añade los propios certificados y listas de Revocación a los documentos firmados para permitir la verificación en el futuro, incluso si las fuentes originales no estuvieran ya disponibles (Wikipedia, 2013).

XML :

El lenguaje de marcas extensible (*Extensible Markup Language*) es un sistema estándar de codificación de información, los programas que utilizan este formato, pueden intercambiar de forma sencilla sus datos debido a una misma lógica interna (zonaClic).

XML-DSIG:

Firma XML (también llamado XMLDsig, DSig XML, XML-Sig) es una recomendación del W3C que define una sintaxis XML para la firma digital. Se utiliza para firmar datos o recursos de cualquier tipo; cualquier cosa que sea accesible a través de una URL puede firmarse (Wikipedia 2014).

3 Firma Digital

Históricamente las personas han utilizado la firma manuscrita como medio para dar fe de la aceptación, autorización o autoría de un documento en papel. Esta actividad se ha mantenido a lo largo de mucho tiempo e impacta la vida privada y laboral de las personas.

Con el avance de la tecnología se ha dado un gran salto en el campo del comercio, la industria y nuevos servicios electrónicos (redes sociales, comercio electrónico, blogs, foros, entre otros) en los cuales las personas se registran e interactúan entre ellas.

Esta interacción entre las personas, utilizando medios digitales y no físicos, ha permitido la disminución de papelería en los trámites financieros, legales, artísticos; y mayor aceptación en realizar "transacciones" de forma electrónica.

Por lo anterior, la necesidad de contar con medios electrónicos para verificar la autoría de la persona que realiza una transacción, es cada vez más necesario, garantizando los trámites efectuados en Internet.

Así "el concepto de firma digital nace de una oferta tecnológica para acercar la firma manuscrita (ológrafa) a lo que se llama el trabajo en redes o ciberespacio que garantiza los trámites hechos en Internet"[1].

Dicho concepto se introdujo en 1976 por Diffie y Hellman[2] en donde la firma digital se conceptualizó como un conjunto de datos que se asocian a un mensaje para dar la validez de identidad de la persona que envió el mensaje y la integridad del mensaje propiamente.

La firma digital ha venido evolucionando y mejorando su funcionalidad, fue en 1995 donde se establece la primera ley en materia de firma digital denominada "*Utha Digital Signature Act*"[3] .

La firma digital en Costa Rica nace por la ley 8454 con el nombre de "Ley de Certificados, Firmas Digitales y Documentos Electrónicos" aprobada el 22 de agosto del 2005.

En esta ley se establece que la firma digital "es un método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. La firma digital del documento es el resultado de aplicar algoritmos matemáticos, (denominados función hash), a su contenido y, generando una firma digital del documento.

1 http://www.firma-digital.cr/que_es/antecedentes.aspx
2 http://www.ia.urjc.es/cms/sites/default/files/userfiles/file/SEG-I/2012/s4xClavePublica%282%29.pdf
3 http://www.firma-digital.cr/que_es/antecedentes.aspx

Ilustración 1
Firmado de un documento

Para verificar la firma se tiene que validar la vigencia del Certificado Digital del firmante, el estado del certificado digital (si está revocado) y que el uso del certificado digital sea el apropiado para la operación realizada (firma y no repudio)[4]."

Dentro de esta definición se presentan dos etapas que tiene la firma digital, a saber:

1. Firmar un documento: requiere un certificado digital emitido por una autoridad certificadora registrada en Costa Rica. Dicho certificado puede estar almacenado y custodiado en un dispositivo (token o tarjetas inteligentes *-smart cards-*).

2. Validar un documento: realiza la vigencia del certificado digital cuando se aplicó la firma digital al documento, además de las validaciones de revocación.

A continuación se da una breve explicación de estas etapas.

FIRMAR DOCUMENTO

1. La persona que desea firmar el documento electrónico, debe abrir el documento y buscar dentro del editor de texto la opción de firmar digitalmente el documento.

2. La aplicación solicitará el medio donde está almacenado la firma de la persona (tarjeta inteligente).

3. La aplicación solicitará los datos de activación "pin" para el acceso a los datos de la persona firmante.

4. La persona firmante ingresa el "pin" el cual es una clave secreta que **únicamente** debe ser conocida por la persona firmante.

4 https://www.firmadigital.go.cr/firma.html

Ilustración 2
Validez de Firma

5. La aplicación calcula el valor del documento mediante algoritmos de encriptación (`MD5 o SHA1`) el cual se denomina digesto y lo encripta mediante la llave privada (clave privada). Adicionalmente la aplicación consulta el estado del certificado con el fin de validar que no esté revocado o suspendido.

La aplicación toma la información generada anteriormente y genera el documento firmado, el cual conforma el documento electrónico, certificado digital, digesto encriptado e información de validación del certificado digital.

VALIDACIÓN DE UN DOCUMENTO FIRMADO

1. Del documento firmado se extrae el documento original y se calcula el valor del documento mediante algoritmos de encriptación (`MD5 o SHA1`) para obtener el digesto.

2. Se extrae del documento firmado el digesto encriptado y el certificado del firmante (que contiene la llave pública, únicamente del firmante).

3. Se des-encripta el digesto con la llave pública del firmante, obteniendo el digesto que se generó cuando se firmó el documento.

Se compara el digesto del paso 1 con el del paso 3. Si son idénticos, la firma es válida, ver ilustración 2.

Adicionalmente, dentro del proceso de validación se revisa que el certificado del firmante sea confiable a saber:

1. Que se haya usado un certificado con capacidad de firma y no repudio.

2. Que el certificado no esté vencido.

3. Que el certificado no esté revocado.
4. Que el certificado haya sido emitido por una autoridad certificadora reconocida.
5. Que los datos del certificado cumplan las políticas de la autoridad certificadora.

4 Instalación del componente de firma digital para LibreOffice

4.1 REQUISITOS

Para la instalación del componente de firma avanzada para LibreOffice debe de contar con:

1. **Certificados y controlador de la tarjeta criptográfica:** el equipo debe contar con los certificados válidos y el controlador de la tarjeta para que sea reconocida en el equipo, para esto puede consultar al sitio web: https://www.soportefirmadigital.com/sfd/dl.aspx?cardid

En caso de dificultad, llamar al teléfono (506) **2528-4949** del Centro de Soporte de Firma Digital.

2. **Java:** debe tener instalado la versión `Open JRE Java 7` para Linux, según la arquitectura de la máquina.
3. **Herramienta ofimática LibreOffice u OpenOffice.**

4.2 INSTALACIÓN DE LIBREOFFICE

Para la instalación de LibreOffice en el equipo donde se usará firma digital avanzada se deben realizar los siguientes pasos:

1. Acceda a una terminal de consola del equipo.
2. Ejecute el comando "`sudo apt-get remove -- purge libreoffice*`" este se encargará de eliminar todos los paquetes relacionados a LibreOffice. Esto tiene la finalidad de hacer una instalación de la versión actualizada de esta herramienta de ofimática.

3. Descargue el LibreOffice actualizado del sitio web: "http://www.libreoffice.org/download".

4. Con la terminal de consola, acceda al directorio de Descargas y desempaque el archivo descargado con el comando "`tar -xvf LibreOffice*`". También puede descomprimirlo desde el navegador de archivos, dando clic derecho sobre el archivo y seleccionando "extraer aquí".

5. En la terminal de consola, acceda al directorio desempacado y dentro de este al directorio"`DEBS`" con el comando "`cd DEBS`".

6. Ejecute el comando "`sudo dpkg -i *.deb`" el cual se encargará de realizar la instalación del LibreOffice.

De esta forma, la nueva versión del LibreOffice estará instalada en el directorio "`/opt`" del computador.

4.3 LIBRERÍA JSS DE MOZILLA FIREFOX

Antes de iniciar la instalación de librerías, es requisito tener instalado el ambiente `Open JRE Java 7` en la máquina que ejecutará el componente para Firma Digital.

Es necesario descargar los archivos `libjss3.so` y `jss33.jar` [5] según la arquitectura (32 bits o 64 bits) del equipo.

Ingrese al sitio web www.ci.ucr.ac.cr/firmadigital para descargar el material correspondiente.

Realice los siguientes pasos:

1. Abra una terminal de consola y sitúese en el directorio donde realizó la descarga de la librería jss, o bien sitúese en el navegador de archivos.

2. Desempaque el archivo según la arquitectura del equipo desde la terminal de consola, ver Ilustración 3. Si desea hacerlo desde el navegador de archivos, haga clic derecho al archivo y seleccione "extraer aquí".

---

5 http://www.mozilla.org/projects/security/pki/jss/javadoc/org/mozilla/jss/CryptoManager.html

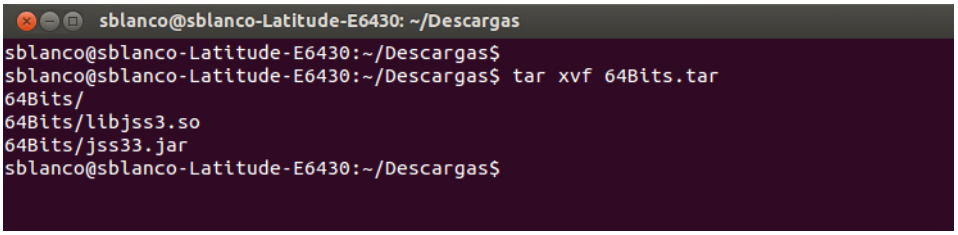

Ilustración 3 Desempacar librerías

3. En la misma terminal de consola ingrese como usuario root, utilizando el comando "`sudo nautilus`" donde el sistema le solicitará la contraseña del usuario `root` en caso de ser necesario, ver Ilustración 4.

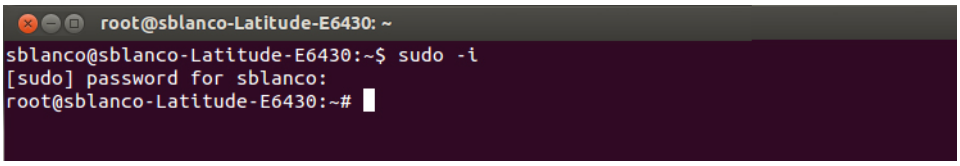

Ilustración 4 Ingreso de contraseña del usuario root

4. Abra la carpeta descargada de las librerías en el navegador de archivos y copie el archivo "`jss33.jar`", según la arquitectura de su computador, en la siguiente dirección de carpetas: "`/usr/lib/jvm/java-7-openjdk/jre/lib/ext`".

5. Vuelva a la carpeta "`jre/lib`" y a la carpeta "`amd64`" o "`i386`" (según la arquitectura de su computador) y copie el archivo "`libjss3.so`" (ubicado en la carpeta de la librería descargada).

6. En la terminal de consola, ingrese al directorio "`/usr/lib/jvm/java-7-openjdk/jre/lib/amd64`" con el comando "`cd/usr/lib/jvm/java-7-openjdk/jre/lib/amd64`". Una vez dentro del directorio escriba el comando "`sudo chmod755 libjss3.so`" para establecer los permisos a esta librería, ver Ilustración 5.

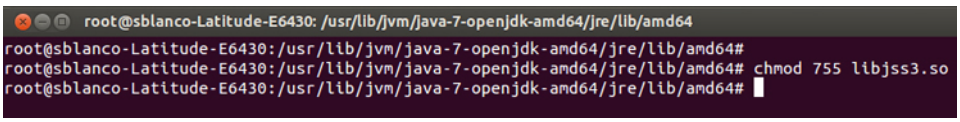

Ilustración 5 Asignación de permisos

7. Acceda al directorio "`/usr/lib/jvm/java-7-openjdk-amd64/jre/lib/ext `" con el comando "`cd /usr/lib/jvm/java-7-openjdk-amd64/jre/lib/ext `" y copie el archivo "`jss33.jar`" con el comando "`cp`". Por

último, asigne permisos ejecutando el comando "`chmod 755 jss33.jar`", ver ilustración 6.

Ilustración 6 Copia de librerías adicionales

4.4 INSTALACIÓN DEL COMPONENTE

A continuación se describen los pasos para la instalación del componente de firma avanzada de LibreOffice en ambiente Linux.

1. Valide que LibreOffice utiliza la versión `JRE 7` de Java.

    1. Acceda a "Herramientas" del menú principal de LibreOffice y seleccione "Opciones" , ver ilustración 7.

    2. Donde se muestra la ventana de las opciones generales, extienda la pestaña de LibreOffice y seleccione la opción de "Avanzado". Se mostrarán los entornos de ejecución de Java instalados donde debe seleccionar la versión 7 , ver ilustración 8.

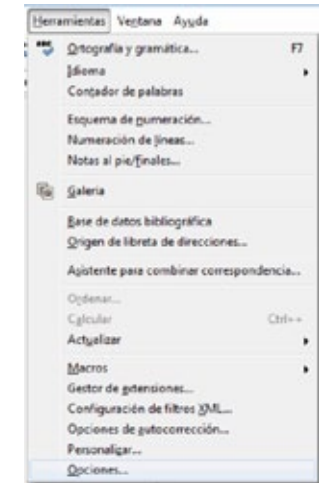

Ilustración 7
Menú Herramientas LibreOffice

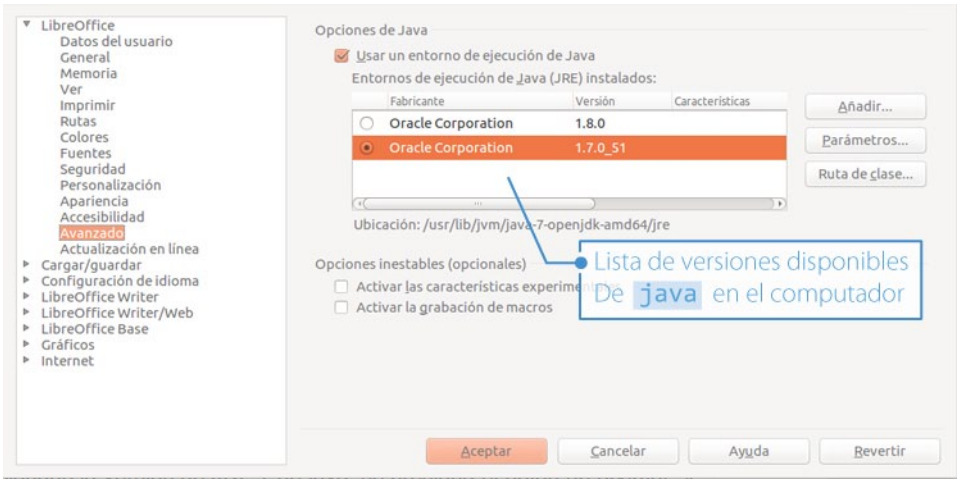

Ilustración 8 Opciones avanzadas de LibreOffice

    3. Ya teniendo seleccionado la versión de `JRE 7 de java`, presione el botón de aceptar.

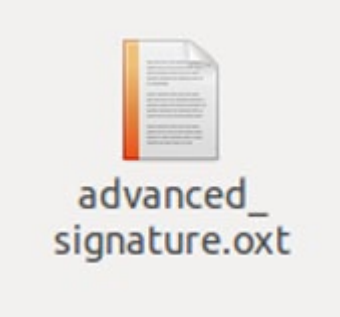

Ilustración 9
Archivo de instalación del componente de firma digital para LibreOffice

2. Descargue el instalador del componente en el sitio web: www.ci.ucr.ac.cr/firmadigital y descargue el componente de LibreOffice, cuyo nombre de archivo corresponde a "`advanced_signature.oxt`", ver ilustración 9.

3. Una vez descargado, abra el archivo (haciendo doble click en el icono) e inicie la instalación de la extensión "Firma digital avanzada XADES X-L". En esta ventana presione el botón de aceptar para iniciar el proceso de instalación o en cancelar si no desea instalar el componente, ver ilustración 10.

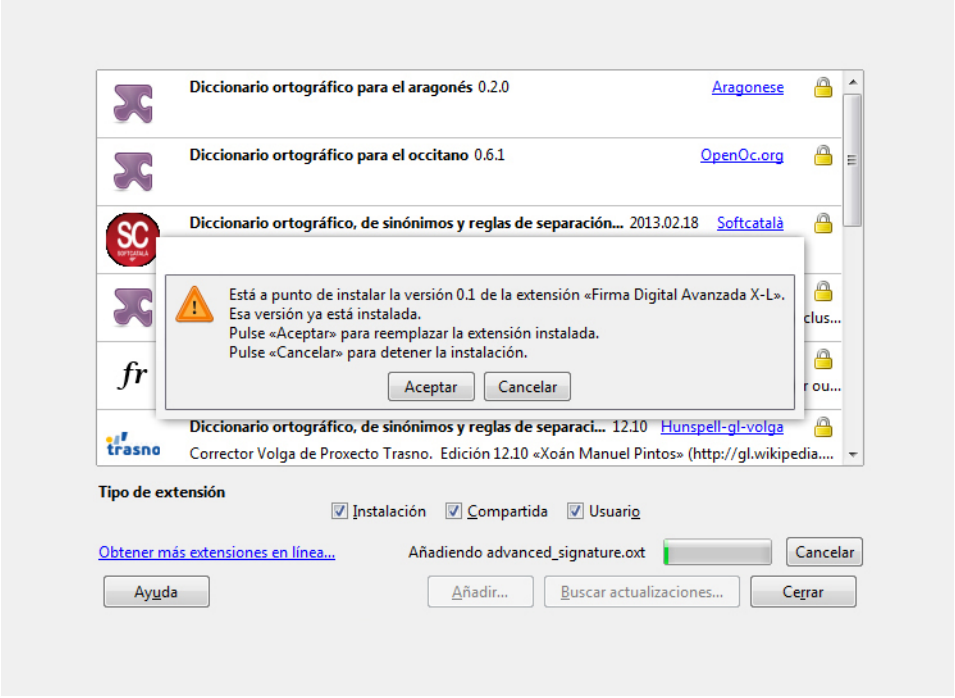

Ilustración 10 Aceptar la instalación

4. Al aceptar, se abrirá la ventana de los términos de licenciamiento. Realice una lectura del licenciamiento del componente y una vez leído y comprendido las condiciones de licenciamiento, debe presionar el botón aceptar en caso de estar de acuerdo, ver ilustración 11.

5. Al aceptar, se inicia la instalación del componente. El proceso puede durar unos segundos. Una vez finalizado, presione el botón cerrar, ver ilustración 12.

6. Una vez cerrada la ventana anterior se abrirá LibreOffice con la nueva pestaña de "Firma Digital" en el menú principal de LibreOffice, ver Ilustración 13.

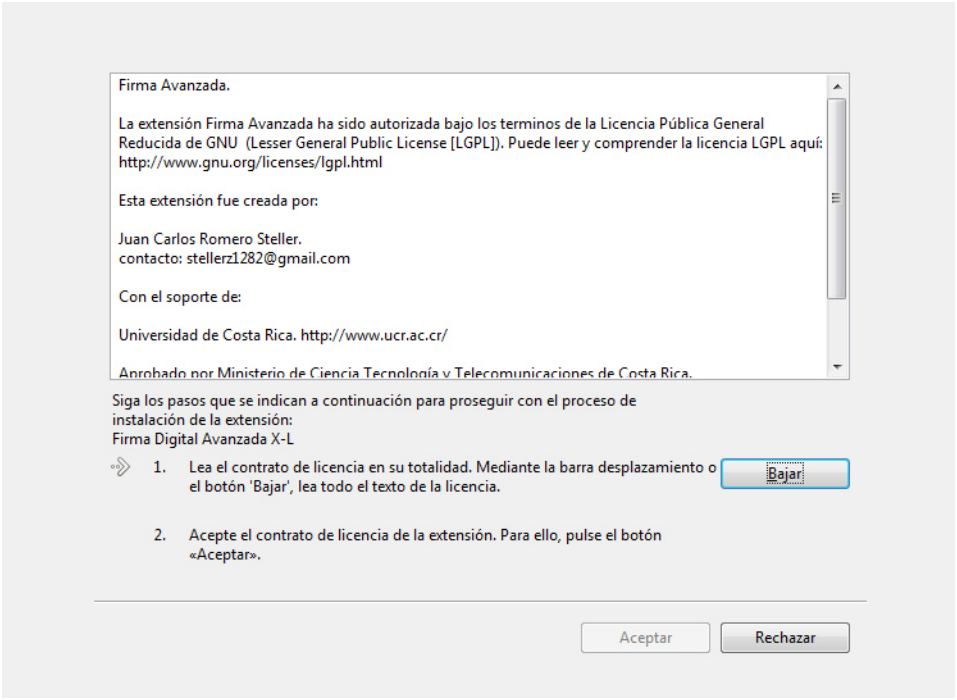
Firma Avanzada.
La extensión Firma Avanzada ha sido autorizada bajo los terminos de la Licencia Pública General Reducida de GNU (Lesser General Public License [LGPL]). Puede leer y comprender la licencia LGPL aquí: http://www.gnu.org/licenses/lgpl.html
Esta extensión fue creada por:
Juan Carlos Romero Steller.
contacto: stellerz1282@gmail.com
Con el soporte de:
Universidad de Costa Rica. http://www.ucr.ac.cr/
Aprobado por Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica.
Siga los pasos que se indican a continuación para proseguir con el proceso de instalación de la extensión:
Firma Digital Avanzada X-L
1. Lea el contrato de licencia en su totalidad. Mediante la barra desplazamiento o el botón 'Bajar', lea todo el texto de la licencia.
Bajar
2. Acepte el contrato de licencia de la extensión. Para ello, pulse el botón «Aceptar».
Aceptar
Rechazar

Ilustración 11 Aceptar la licencia del nuevo componente

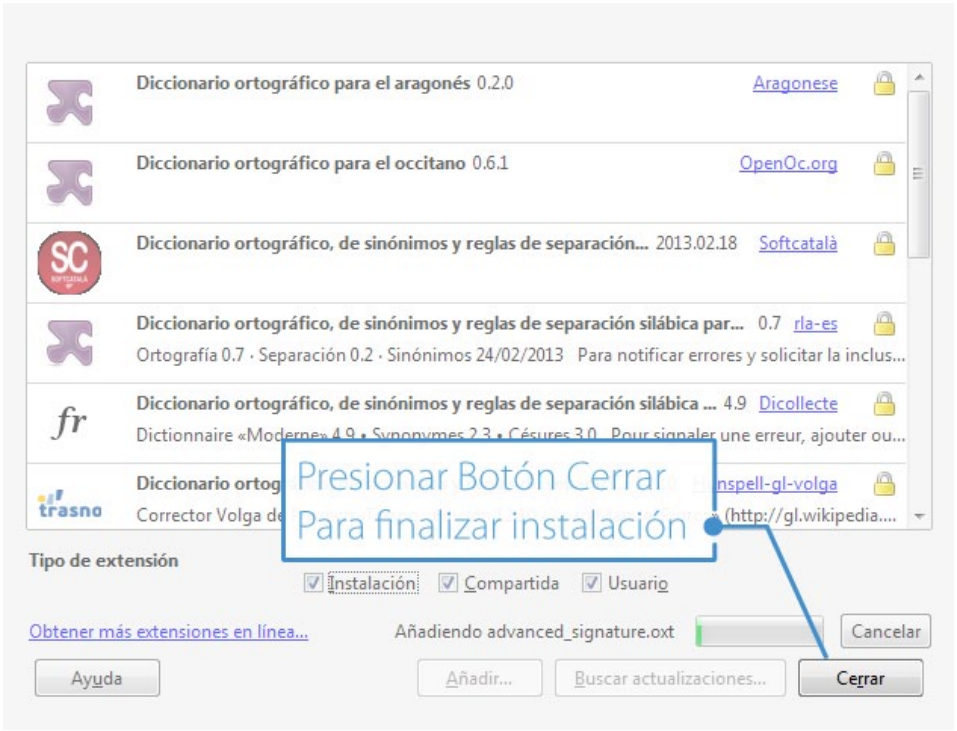
Diccionario ortográfico para el aragonés 0.2.0 Aragonese
Diccionario ortográfico para el occitano 0.6.1 OpenOc.org
Diccionario ortográfico, de sinónimos y reglas de separación... 2013.02.18 Softcatalà
Diccionario ortográfico, de sinónimos y reglas de separación silábica par... 0.7 rla-es
Ortografía 0.7 · Separación 0.2 · Sinónimos 24/02/2013 Para notificar errores y solicitar la inclus...
Diccionario ortográfico, de sinónimos y reglas de separación silábica ... 4.9 Dicollecte
Presionar Botón Cerrar
Para finalizar instalación
Tipo de extensión
Instalación
Compartida
Usuario
Obtener más extensiones en línea...
Añadiendo advanced_signature.oxt
Cancelar
Ayuda
Añadir...
Buscar actualizaciones...
Cerrar

Ilustración 12 Espera de la instalación el componente

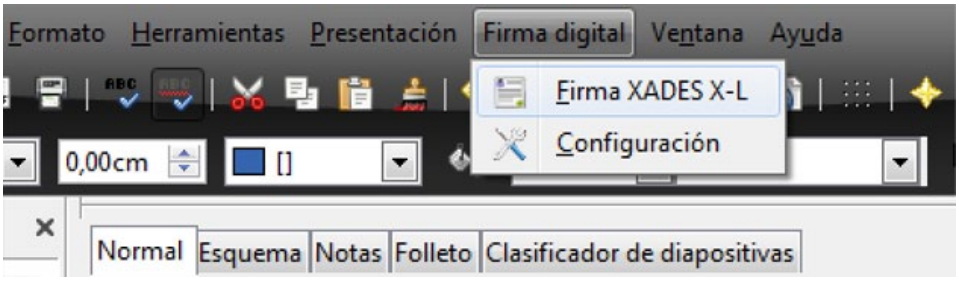

Ilustración 13 Nuevo menú en la barra de menú principal de LibreOffice

5 Firma avanzada con formato "XADES X-L"

A continuación se presentan los pasos para aplicar firma avanzada en documentos con formato ODF (*OpenDocument Format*) y su respectiva verificación. En la siguiente tabla se indican las extensiones de cada tipo de documento en el que se puede aplicar firma digital avanzada.

DOCUMENTO	EXTENSIÓN
Texto (Writer)	.odt
Hoja de cálculo (Calc)	.ods
Presentación (Impress)	.odp
Dibujo (Draw)	.odg

Tabla #1
Extensiones de documentos OpenDocument.

5.1 FIRMAR UN DOCUMENTO

Para poder aplicar la firma digital a un documento en LibreOffice, es necesario que solamente esté el documento abierto, y dejar cerrado cualquier otro documento de LibreOffice que no se va a firmar.

A continuación se describe el proceso para aplicar la firma digital avanzada a un documento.

1. Abra el documento que desea firmar, si este se encontraba editando y no se ha guardado no se podrá aplicar la firma digital, por lo que es necesario que el documento esté previamente guardado.

2. Seleccione en el menú principal la pestaña de “Firma Digital” y dentro de este, la opción “`Firma XADES X-L`”, ver Ilustración 14.

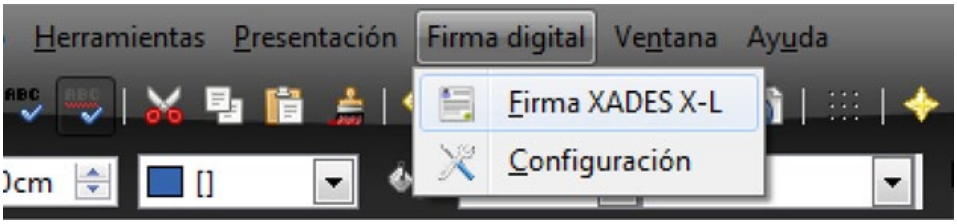

Ilustración 14 Selección firma XADES X-L

3. Una vez seleccionado se mostrará la ventana de firmas digitales, presione en el botón “Firmar documento”, ver la Ilustración 15.

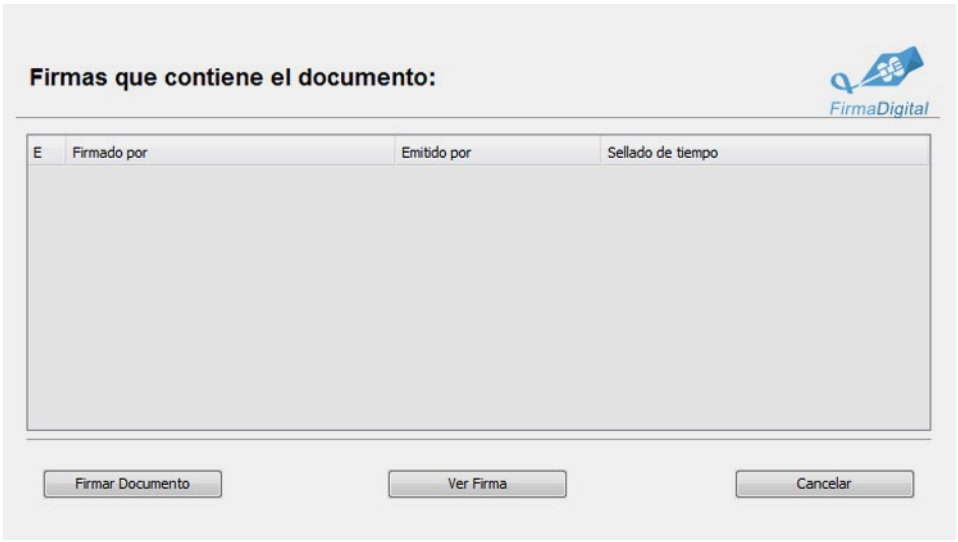

Ilustración 15 Ventana principal de Firma Digital

4. Esta opción despliega una ventana de diálogo donde debe ingresar el “pin” de la tarjeta inteligente para tener acceso a los certificados, ver Ilustración 16.

5. Si la clave es correcta se abrirá la ventana para la selección de los certificados para firmar. Seleccione el certificado digital que desea utilizar para firmar el documento y presione el botón “Aceptar”, ver Ilustración 17.

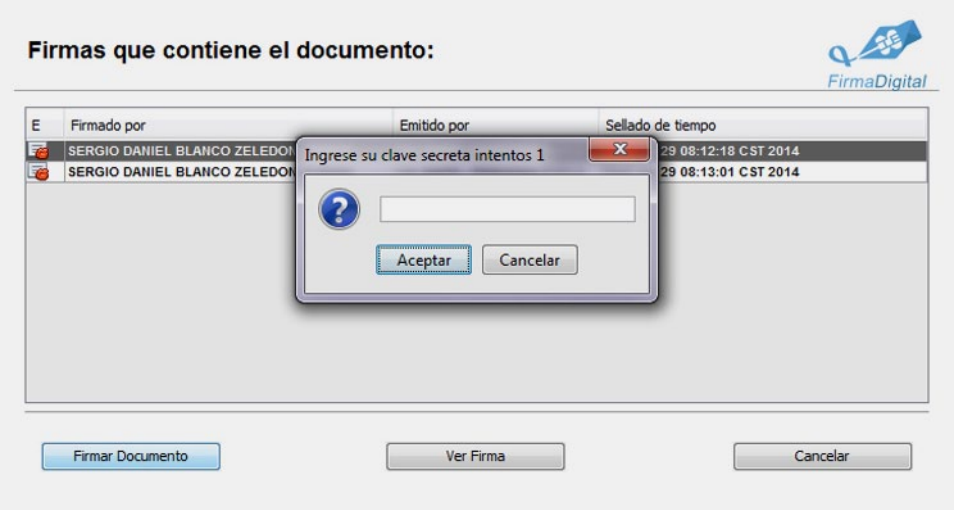

Ilustración 16 Diálogo para ingresar la clave privada de desbloqueo de la tarjeta criptográfica

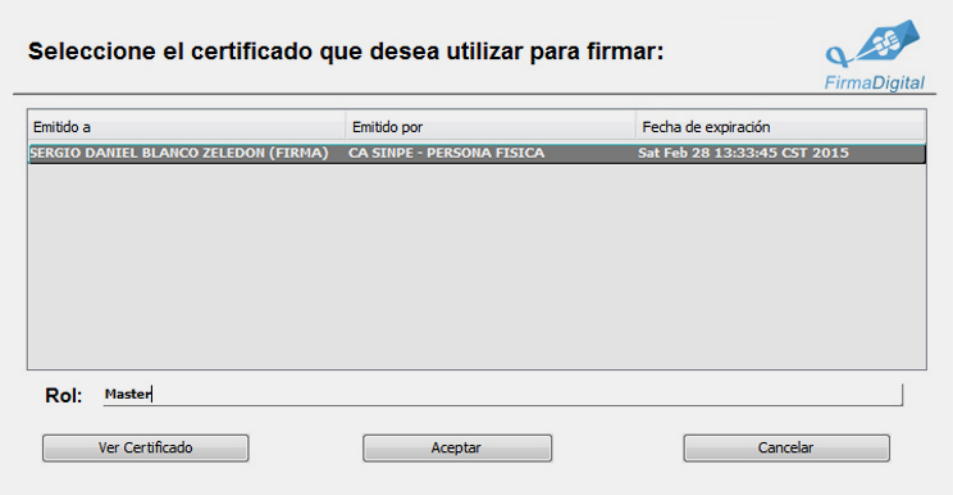

Ilustración 17 Ventana de selección del certificado para firmar

Si no se lista el certificado digital, puede ser por dos razones:

- No se tienen instalados los certificados como lo establecen los requerimientos en el presente documento.
- La tarjeta no está bien conectada en el lector, para esto deberá de asegurarse que este bien conectada y cerrar por completo el LibreOffice y abrirlo nuevamente.

6. Mientras se firma el documento, se abrirá una ventana donde se muestra una barra de proceso y luego despliega las acciones que se realizan para la firma del documento, ver Ilustración 18.

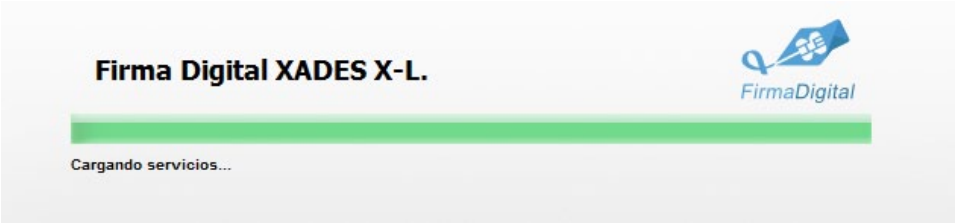

Ilustración 18 Ventana de espera mientras se firma el documento

7. Al finalizar el proceso se muestra una ventana que indica la ruta donde almacenó el documento ya aplicada la firma digital.

El nombre del documento, será el mismo que el original, agregando el prefijo "`Signed_`", ver Ilustración 19. Presione el botón "Aceptar" y volverá a la ventana anterior donde debe presionar el botón de "Cancelar" para cerrar la ventana.

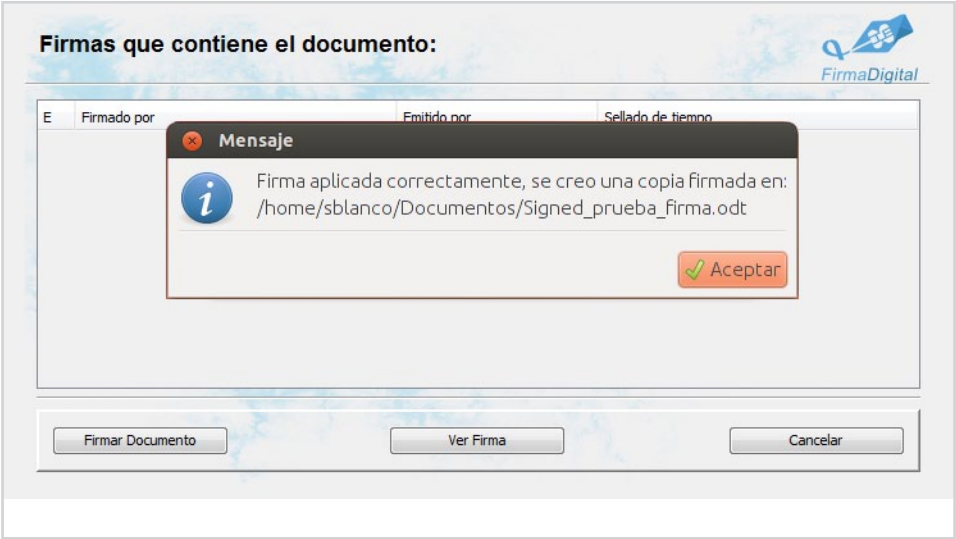

Ilustración 19 Notificación de aplicación de firma digital

8. De esta forma ya se aplicó la firma avanzada al documento y para verlo basta solo con abrir el documento "`Signed_ + <nombre_documento>`" en LibreOffice.

5.2 VERIFICAR FIRMA

En esta sección se mostrará la forma de verificar la firma de un documento con formato ODF. Adicionalmente, se describen opciones que permiten ver el contenido de la firma y demás certificados que se manejan.

5.2.1 VERIFICACIÓN GENERAL

A continuación se detalla los pasos para la verificación de un documento.

1. Al abrir un documento firmado, el LibreOffice validará la firma y mostrará el resultado mediante un símbolo en la barra de estado, ver Ilustración 20.

Ilustración 20 Barra de estado de LibreOffice indica y valida una firma digital

Si no aparece el símbolo, revise que el computador, donde se esta realizando la verificación de la firma, cuente con los certificados de la entidad certificadora, requisito establecido al inicio del documento.

En la siguiente tabla se describen los distintos tipos de iconos que se representan en el manejo de firma digital.

SÍMBOLO EN BARRA DE ESTADO	ESTADO DE FIRMA
	La firma es válida.
	La firma es correcta, pero no se han podido validar los certificados. La firma y el certificado son correctos, pero no se han firmado todas las partes del documento. (Para los documentos que se han firmado con versiones antiguas de este software, consulte la nota siguiente).
	La firma no es válida.

Tabla #2 Extensiones de documentos OpenDocument[6]

6 https://www.soportefirmadigital.com/sfd/fd.aspx?cardid=

5.2.2 VERIFICACIÓN DETALLADA

Para ver el detalle de la firma digital avanzada :

1. Abra un documento firmado.

2. Acceda en el menú principal a “Firma Digital”y a la opción “Firma XADES X-L” la cual desplegará la ventana listando las firmas que tiene el documento registradas, ver ilustración 21.

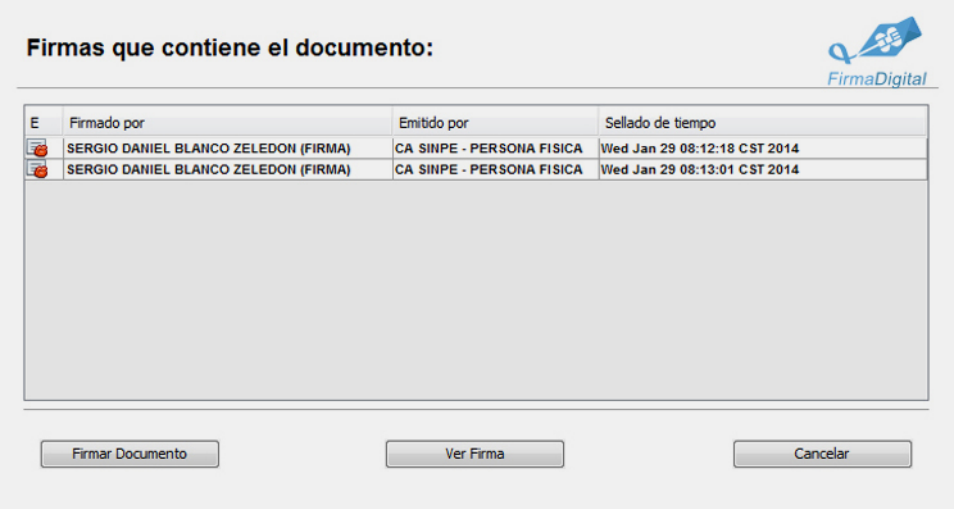

Ilustración 21 Ventana principal de Firma Digital, vista de un documento firmado anteriormente

3. Para ver información detallada sobre la firma, seleccione una firma de la lista y presione el botón “**Ver Firma**”, Este abrirá una ventana donde se detalla la información de la firma digital seleccionada, ver ilustración 22.

Esta ventana muestra la información que contiene la firma XADES X-L, como es:

1. Nombre del firmante.

2. Rol establecido por el firmante.

3. Validación de toda la cadena de certificados mediante protocolo CRL

4. Validación del certificado de firma mediante protocolo OCSP.

Si al abrir una firma, un certificado era inválido al momento de firmar los campos de validación CRL y OCSP, mostrarán un mensaje de certificado inválido.

Ilustración 22 Ventana de detalle de un firma digital seleccionada

5.2.3 VER XML DE LA FIRMA DIGITAL

Otro dato importante de la validación de una firma digital es poder ver la estructura interna de una firma digital avanzada, y verificar que esta cuenta con todos los componentes adecuados para que cumpla con el estándar XADES X-L.

El componente le permite ver la firma digital en formato XML, el cual representa la estructura interna de la firma que realizó el usuario.Para ver esta información, presione el botón "Ver XML" de la ventana de detalle de la firma digital, ver ilustración 23, el cual abrirá la ventana de vista XML donde podrá validar la estructura interna de la firma, ver ilustración 23.

Adicionalmente de la validación de la estructura interna de la firma, se puede observar en detalle los datos contenidos en un certificado digital usado para firmar, principalmente la cadena de certificados que respaldan al certificado de firma, así como los datos generales de cada certificado.

Para ver esta información presione el botón "Ver Certificado" de la ventana de detalle de la firma digital, ver ilustración 23, el cual abrirá la ventana donde se desglosa la cadena de certificados de la firma digital con sus propiedades, ver ilustración 24.

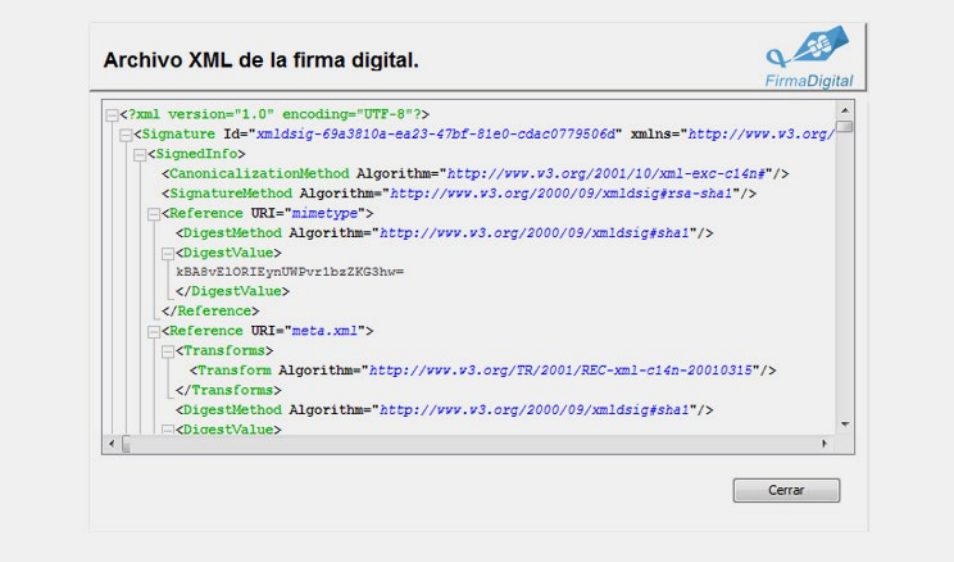

Ilustración 23 Ventana ver XML, para ver la estructura interna de la firma digital

Ilustración 24 Ventana de información de los certificados digitales

6 Jerarquía Nacional de Certificados

Hay que tener presente la Jerarquía Nacional de certificados para comprobar la procedencia del certificado que firma el documento. En la Ilustración 25 se muestra la Jerarquía Nacional de Certificados de Costa Rica.[7]

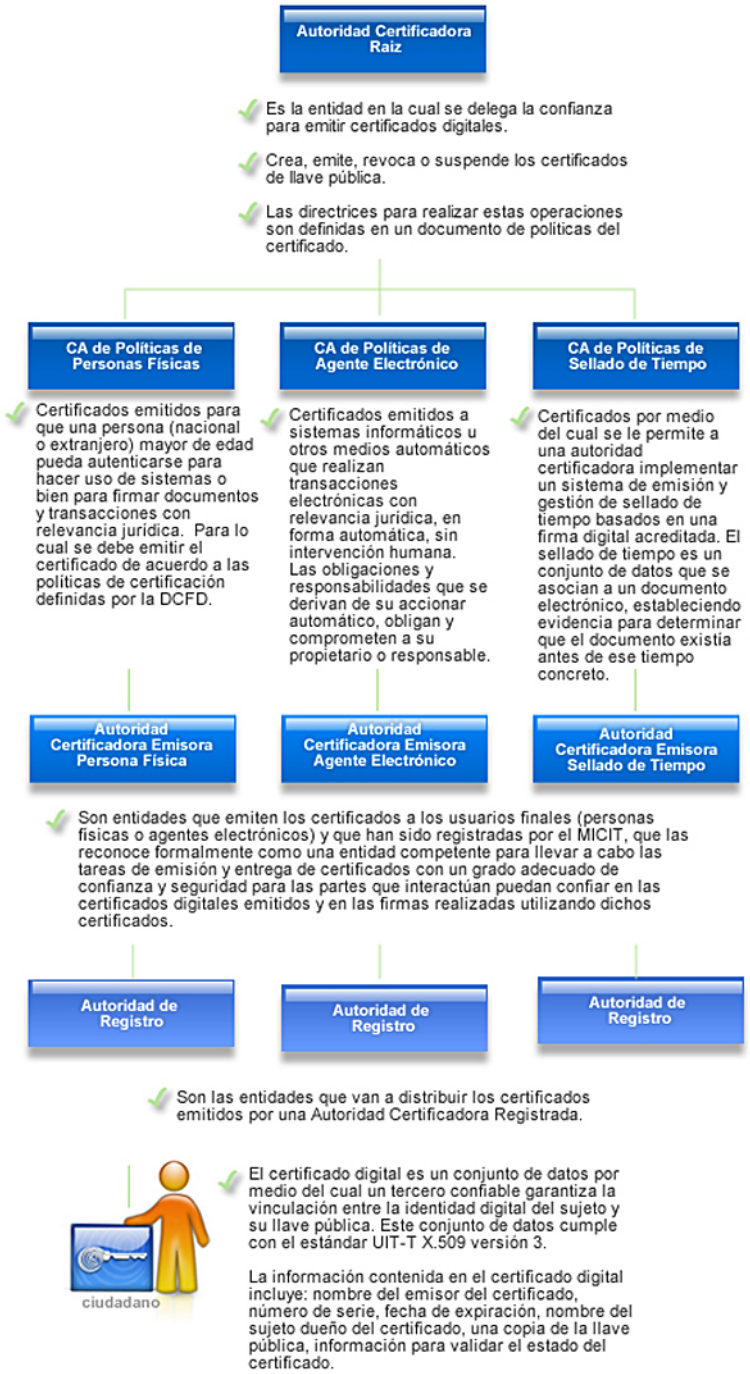
Autoridad Certificadora Raiz
Es la entidad en la cual se delega la confianza para emitir certificados digitales.
Crea, emite, revoca o suspende los certificados de llave pública.
Las directrices para realizar estas operaciones son definidas en un documento de políticas del certificado.
CA de Políticas de Personas Físicas
CA de Políticas de Agente Electrónico
CA de Políticas de Sellado de Tiempo
Certificados emitidos para que una persona (nacional o extranjero) mayor de edad pueda autenticarse para hacer uso de sistemas o bien para firmar documentos y transacciones con relevancia jurídica. Para lo cual se debe emitir el certificado de acuerdo a las políticas de certificación definidas por la DCFD.
Certificados emitidos a sistemas informáticos u otros medios automáticos que realizan transacciones electrónicas con relevancia jurídica, en forma automática, sin intervención humana. Las obligaciones y responsabilidades que se derivan de su accionar automático, obligan y comprometen a su propietario o responsable.
Certificados por medio del cual se le permite a una autoridad certificadora implementar un sistema de emisión y gestión de sellado de tiempo basados en una firma digital acreditada. El sellado de tiempo es un conjunto de datos que se asocian a un documento electrónico, estableciendo evidencia para determinar que el documento existía antes de ese tiempo concreto.
Autoridad Certificadora Emisora Persona Física
Autoridad Certificadora Emisora Agente Electrónico
Autoridad Certificadora Emisora Sellado de Tiempo
Son entidades que emiten los certificados a los usuarios finales (personas físicas o agentes electrónicos) y que han sido registradas por el MICIT, que las reconoce formalmente como una entidad competente para llevar a cabo las tareas de emisión y entrega de certificados con un grado adecuado de confianza y seguridad para las partes que interactúan puedan confiar en las certificados digitales emitidos y en las firmas realizadas utilizando dichos certificados.
Autoridad de Registro
Autoridad de Registro
Autoridad de Registro
Son las entidades que van a distribuir los certificados emitidos por una Autoridad Certificadora Registrada.
ciudadano
El certificado digital es un conjunto de datos por medio del cual un tercero confiable garantiza la vinculación entre la identidad digital del sujeto y su llave pública. Este conjunto de datos cumple con el estándar UIT-T X.509 versión 3.
La información contenida en el certificado digital incluye: nombre del emisor del certificado, número de serie, fecha de expiración, nombre del sujeto dueño del certificado, una copia de la llave pública, información para validar el estado del certificado.

Ilustración 25
Jerarquía Nacional de Certificados Digitales

7 http://www.firmadigital.go.cr/jerarquia.html

7 Configuración del componente de firma digital

El componente cuenta con una configuración que permite personalizar parámetros y ver información del mismo.

Para esto se debe acceder a la opción de "Configuración" que se encuentra en el menú de "Firma Digital", ver Ilustración 26.

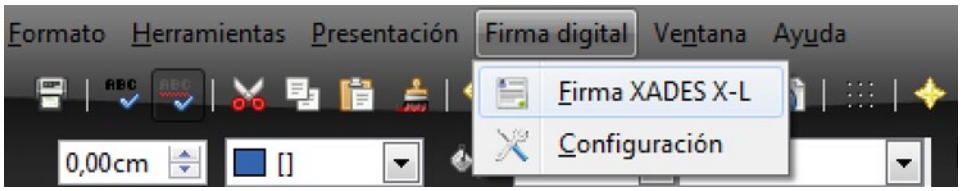

Ilustración 26 Menú principal del componente de firma digital

Una vez seleccionada la opción se despliega la ventana que se aprecia en la Ilustración 27.

Ilustración 27 Ventana de configuración del componente de firma digital

En dicha ventana se muestran tres campos de información a saber:

1. **URL de TSA:** especifica el `URL` del servidor de sellado de tiempo. Este servidor permite que durante el proceso de firma digital, el componente envíe una consulta de sellado de tiempo el cual devuelve un certificado y el tiempo donde se recibió la solicitud, dando certeza de la hora en que se efectuó la firma del documento. Para el caso de Costa Rica se utiliza el servicio proporcionado por el Banco Central en la dirección `URL`: "http://tsa.sinpe.fi.cr/tsaHttp/", este es un servicio abierto y gratuito.

2. **Ruta driver de la tarjeta:** informa sobre la ruta del controlador de la tarjeta criptográfica. Este controlador se instala cuando se realiza la instalación de los certificados digitales. Por ejemplo, en el sistema Operativo Windows este dato es instalado en la ruta: "`C:\Windows\System32\asepkcs.dll`" y el archivo se llama "`asepkcs.dll`".

3. **Rol del firmante:** identifica el rol del firmante que tendrá al firmar documentos, pueden ser datos como: Firmante, Analista, Co-firmante, Colaborador, etc; o se podría usar para definir el rango profesional del firmante por ejemplo: Bachiller, Licenciado, Máster o Doctor, etc; se deja al gusto del usuario o la empresa, también se podría dejar vació ya que no influye en el funcionamiento de la aplicación.

En la parte inferior de esta ventana se encuentran tres botones, los cuales se detallan a a continuación:

1. Restaurar: permite establecer los valores iniciales de la instalación del componente. Por ejemplo, si cambia el URL del sellado de tiempo y desea recuperar el valor "`default`", al presionar este botón el componente sustituirá la información de este campo con el valor inicial.

2. Guardar: guarda los datos que han sido modificados.

3. Cerrar: cierra la ventana sin guardar la información que haya sido modificada.

8 Errores

1. ERROR 1: SE DESPLIEGA MENSAJE, VER ILUSTRACIÓN 28

Es debido a dos situaciones:

1. Cuando se mantiene por un largo tiempo, la ventana donde se muestra la lista de certificados a seleccionar para aplicar la firma.
2. Se cuenta con más de una ventana del LibreOffice abierta.

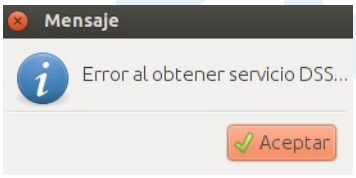

Ilustración 28
Error en el manejo de la Firma avanzada

2. ERROR 2: SE DESPLIEGA MENSAJE, VER ILUSTRACIÓN 29

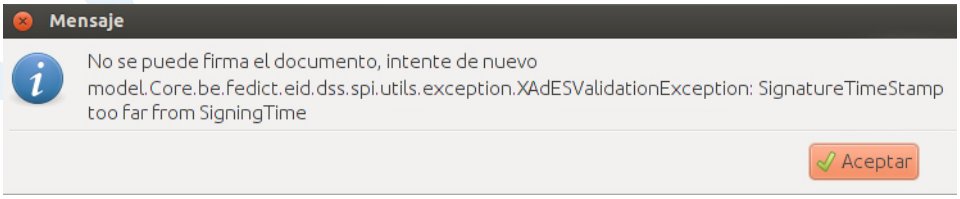
Mensaje
No se puede firma el documento, intente de nuevo
model.Core.be.fedict.eid.dss.spi.utils.exception.XAdESValidationException: SignatureTimeStamp too far from SigningTime
Aceptar

Ilustración 29 Error por problemas de la zona horaria registrada en el computador

Esta situación se presenta cuando el computador donde se está aplicando la firma tiene una zona horaria que no corresponde.

Solución:

Ajuste el computador en la zona horaria del país, por ejemplo en Costa Rica la zona horaria es "UTC- 6:00 America Central".

9 Referencias bibliográficas

Firma Digital de Costa Rica http://www.firma-digital.cr/que_es/antecedentes.aspx

Soporte firma digital Costa Rica https://www.soportefirmadigital.com/sfd/

SubSecretaria Poder Judicial Informática de Argentina: http://www.scba.gov.ar/servicios/fdwebn.swf

Universidad Rey Juan Carlos. http://www.ia.urjc.es/cms/

Gobierno de España (2008). Open Document. Recuperado el 2014 de Ministerio de Edicación, Cultura y Deporte; http://recursostic.educacion.es/observatorio/web/ca/software/software-general/660-open-document

Firma Digital.cr (2011) No repudio. Recuperado el 2014, de http://www.firma-digital.cr/como%20funciona/no_repudio.aspx

Martínez, I. (2013). Qué es MD5, cómo funciona y para qué se usa. Recuperado el 2014, de Rootear: http://rootear.com/seguridad/md5-como-funciona-usos

Wikipedia (2014). MD5. Recuperado el 2014, de http://es.wikipedia.org/wiki/MD5

Wikipedia (2013) Xades. Recuperado el 2014, de http://es.wikipedia.org/wiki/Xades

Wikipedia (2014). Firma XML. Recuperado el 2014, de http://es.wikipedia.org/wiki/Firma_XML

Trajtenberg, J. (2002). La firma digital hoy. Recuperado el 2014, de Universidad del Salvador (USAL): www.salvador.edu.ar/ui2-35-trajtenberg.pps (Power Point)

INFORMATICAHOY. (s.f.). Qué es la criptografía. Recuperado el 2014, de http://www.informatica-hoy.com.ar/seguridad-informatica/Criptografia.php

Alcántara, J. (s.f.). Cifrado asimétrico. Recuperado el 2014, de Versvs: http://wiki.versvs.net/Cifrado_asim%C3%A9trico

CATCert. (s.f.). Online Certificate Status Protocol (OCSP). Recuperado el 2014 de http://www.catcert.cat/esl/RECURSOS/Compruebe-su-certificado/Online-Certificate-Status-Protocol-OCSP

Preukschat (2014). ¿Qué es y de qué sirve el algoritmo SHA-256 en el protocolo Bitcoin? – Secure Hash Algorithm (VII). Recuperado el 2014, de OroyFinanzas.com: http://www.oroyfinanzas.com/2014/01/algoritmo-sha-256-protocolo-bitcoin-secure-hash-algorithm/

Banco Santander. (s.f.). Índice de certificados. Recuperado el 2014 de Autoridad Certificadora Banesto; http://ca.banesto.es/ayuda/faqs/generalidades2.html

ZonaClic. (s.f.). ¿Qué es XML?. Recupeado el 2014 de Generalitat de Catalunya: http://clic.xtec.cat/es/jclic/xml.htm

Versión actualizada a junio 2014.

Revisada por el Centro de Informática

Universidad de Costa Rica.